Asymptotically exact heuristics for (near) primitive roots. II

Pieter Moree

Abstract

Let $g \in \mathbb{Q}^*$ be a rational number. Let $N_{g,t}(x)$ denote the number of primes $p \le x$ for which the subgroup of $(\mathbb{Z}/p\mathbb{Z})^*$ generated by g mod p is of residual index t. In [7] an heuristic for $N_{g,t}(x)$ was set up, under the assumption of the Generalized Riemann Hypothesis (GRH), and shown to be asymptotically exact. In this paper we provide an alternative and rather shorter proof of this result.

Keywords: heuristic, residual index, natural density, primitive root.

1 Introduction

Let $g \in \mathbb{Q}\backslash\{-1,0,1\}$ and $t \ge 1$ be an arbitrary natural number. We write $g = \pm g_0^h$, where $g_0 > 0$ is not an exact power of a rational and $h \in \mathbb{Z}_{\ge 1}$. Every prime p in this paper is (mostly tacitly) assumed to be odd and satisfy $\mathrm{ord}_p(g) = 0$, e.g. $\pi(x;t,1)$ denotes the number of odd primes $p \le x$ with $p \equiv 1(\mathrm{mod}\ t)$ and $\mathrm{ord}_p(g) = 0$. We define $r_g(p) = [(\mathbb{Z}/p\mathbb{Z})^* : \langle g \bmod p\rangle]$ and say that $r_g(p)$ is the *residual index mod* p of g. For an arbitrary natural number t we consider the set $N_{g,t}$ of primes p satisfying $r_g(p) = t$ and let $N_{g,t}(x)$ denote the number of primes $p \le x$ in $N_{g,t}$. Notice that $N_{g,1}$ is the set of primes p such that g is a primitive root mod p. In this paper we are interested in the behaviour of $N_{g,t}(x)$ as x tends to infinity. Our heuristic approach to $N_{g,t}(x)$ will be entirely based on a heuristic approach to $R_{g,t}(x)$, which is defined as the number of primes $p \le x$ with $t|r_g(p)$.

Let p be a prime with $p \equiv 1(\mathrm{mod}\ t)$. Note that the density of elements $\gamma \in (\mathbb{Z}/p\mathbb{Z})^*$ such that $r_\gamma(p) = t$ is $\varphi((p-1)/t)/(p-1)$, where φ denotes Euler's totient function. Thus naively one might expect that

$$N_{g,t}(x) \sim \sum_{\substack{p \le x \\ p \equiv 1(\mathrm{mod}\ t)}} \frac{\varphi((p-1)/t)}{p-1} \quad (x \to \infty). \tag{1}$$

Mathematics Subject Classification (2001). Primary 11R45; Secondary 11A07

Despite the fact that for arbitrary $C > 1$ and $m > \exp(4\sqrt{\log x \log\log x})$, we have by [7, Theorem 7],

$$\frac{1}{m}\sum_{g\le m} N_{g,t}(x) = \sum_{\substack{p\le x\\ p\equiv 1(\bmod\ t)}} \frac{\varphi((p-1)/t)}{p-1} + O\left(\frac{x}{\log^C x}\right),$$

and thus the naive heuristic holds true on average, it can be shown on GRH, that (1) is false for many g. In [7], however, the following modified heuristic involving a function $w_{g,t}(p) \in \{0,1,2\}$ was introduced and shown to be asymptotically exact under GRH. (We stipulate that zero multiplied by something not well-defined equals zero. By (a,b) we denote the greatest common divisor of a and b.)

Theorem 1 [7]. *Let $g \in \mathbb{Q}\backslash\{-1,0,1\}$ and $t \ge 1$ be an arbitrary integer. Write $g = \pm g_0^h$, where $g_0 \in \mathbb{Q}$ is positive and not an exact power of a rational and $h \in \mathbb{Z}_{\ge 1}$. Let $d(g_0)$ denote the discriminant of $\mathbb{Q}(\sqrt{g_0})$. Let $2^e || h$ and $2^\tau \mid\mid t$. Put $h_t = h/(h,t)$ and*

$$\epsilon_1 = \begin{cases} 0 & \text{if } \tau < e; \\ -1 & \text{if } \tau = e; \\ 1 & \text{if } \tau > e. \end{cases}$$

If $g > 0$, $p \equiv 1(\bmod\ t)$ and $((p-1)/t, h_t) = 1$, then put

$$w_{g,t}(p) = 1 + \frac{\epsilon_1}{2}\{1 + (-1)^{\frac{p-1}{2^e}}\}\left(\frac{d(g_0)}{p}\right).$$

If $g < 0$, $2 \nmid h_t$, $p \equiv 1(\bmod\ \mathrm{lcm}(2^{e+1}, t))$ and

$$((p-1)/t, h_t) = 1,$$

then put

$$w_{g,t}(p) = 1 + \epsilon_1(-1)^{\frac{p-1}{2^{e+1}}}\left(\frac{d(g_0)}{p}\right).$$

If $g < 0$, $2|h_t$, $p \equiv 1(\bmod\ 2t)$ and $((p-1)/2t, h_t) = 1$, then put $w_{g,t}(p) = 2$. In all other cases put $w_{g,t}(p) = 0$.

Under GRH we have

$$N_{g,t}(x) = (h,t) \sum_{\substack{p\le x\\ p\equiv 1(\bmod\ t)}} w_{g,t}(p)\frac{\varphi((p-1)/t)}{p-1} + O\left(\frac{x\log\log x}{\log^2 x}\right). \tag{2}$$

The purpose of this note is to give a much shorter proof of Theorem 1 than the one given in [7]. The asymptotically exact heuristics developed here for $R_{g,t}(x)$ have further applications, for example in the study of exact heuristics for divisors of recurrences of second order [8].

2 Results of Hooley and Wagstaff

In this section we briefly recall the approach of Hooley and Wagstaff in estimating $N_{g,t}(x)$, cf. [11]; it is analogous to Hooley's [1] break through attack on $N_{g,1}(x)$, the primitive root counting function. The basic observation is that $t|r_g(p)$ iff p splits completely in the splitting field $F_t = \mathbb{Q}(\zeta_t, g^{1/t})$ of the polynomial $X^t - g$ over $\mathbb{Q}$, where $\zeta_t = \exp(2\pi i/t)$. As a consequence (Corollary 1) of the prime ideal theorem, a special case of both the Frobenius and the Chebotarev density theorem, the set of these primes has natural density $1/[F_t : \mathbb{Q}]$. The primes in $N_{g,t}$ are those that do not split completely in any of the fields F_{kt} with $k > 1$. A standard inclusion-exclusion argument readily yields the heuristic value

$$\sum_{k=1}^{\infty} \frac{\mu(k)}{[F_{kt} : \mathbb{Q}]}, \tag{3}$$

for the natural density of the set $N_{g,t}$ (provided that $N_{g,t}$ has indeed a natural density). The sum (3) converges whenever g is different from ± 1, since in that case $[F_{kt} : \mathbb{Q}]$ differs from its 'approximate value' $kt\varphi(kt)$ by a factor that is easily bounded in terms of g, cf. Lemma 7. In fact, we obtain an upper bound for the upper density of the set $N_{g,t}$ in this way. In order to turn this heuristic argument for $N_{g,1}$ into a proof, Hooley employed estimates for the remainder term in the prime number theorem for the fields F_k that are currently only known to hold under GRH. Hooley's arguments are easily extended to $N_{g,t}$ and result in the following theorem.

Theorem 2 (GRH). *Let* $g \in \mathbb{Q}\backslash\{-1, 0, 1\}$ *and* $\mathrm{Li}(x) = \int_2^x \mathrm{d}t/\log t$. *Then*

$$N_{g,t}(x) = A(g,t)\mathrm{Li}(x) + O\left(\frac{x \log\log x}{\log^2 x}\right),$$

where

$$A(g,t) := \sum_{k=1}^{\infty} \frac{\mu(k)}{[\mathbb{Q}(\zeta_{kt}, g^{1/kt}) : \mathbb{Q}]}.$$

Now $A(g,t)$ can be expressed as a linear combination of sums of the form

$$S(h,t,m) := \sum_{\substack{k=1 \\ m|kt}}^{\infty} \frac{\mu(k)(kt,h)}{kt\varphi(kt)}. \tag{4}$$

Each sum $S(h,t,m)$ can be written as an Euler product and in fact is a rational multiple of A, the Artin constant (cf. Lemma 2.1 and Theorem 2.2 of [11]).

3 Proof preview

In this section we sketch the proof of Theorem 1 given in [7] and give a preview of the proof of Theorem 1 to be given in section 6, making also clear the advantages of the new proof over the old one.

We begin by sketching the proof of Theorem 1 given in [7]. Let G be a finite cyclic group of order n, $t|n$ and $\gamma \in G$. We put $f'_{\gamma,t}(G) = 1$ if $[G : \langle\gamma\rangle] = t$ and $f'_{\gamma,t}(G) = 0$ otherwise. It is easy to show that

$$f'_{\gamma,t}(G) = \frac{\varphi(n/t)}{n} \sum_{d|n} \frac{\mu(d/(d,t))}{\varphi(d/(d,t))} \sum_{\mathrm{ord}\chi = d} \chi(\gamma), \tag{5}$$

where the sum is over all multiplicative characters of G of order d. Let us for simplicity assume that $g > 0$. We notice that if $r_g(p) = t$, then $((p-1)/t, h_t) = 1$. Thus

$$N_{g,t}(x) = \sum_{\substack{p \le x \\ (\frac{p-1}{t}, h_t) = 1}} f'_{g,t}((\mathbb{Z}/p\mathbb{Z})^*). \tag{6}$$

In the latter sum we calculate the contribution of the characters $\chi(g_0^h)$ with χ of order d with $d|h$ (the 'linear' contribution) and those χ of order dividing $2h$ but not h (the 'quadratic' contribution). For those in the linear contribution we have $\chi(g) = 1$ and for those in the quadratic we have $\chi(g) = (d(g_0)/p)$. The linear contribution turns out to be equated with the naive heuristic approach and the linear together with the quadratic contribution with a more subtle heuristic approach based on having a priori knowledge of $(d(g_0)/p)$. Working out the contributions of the relevant characters one obtains the sum appearing in (2). In doing so crucial use of the condition $((p-1)/t, h_t) = 1$ is made (note that (6) is also valid when the condition $((p-1)/t, h_t) = 1$ is dropped). The sum in (2) can be unconditionally evaluated with error term $O(x \log^{-C} x)$, with $C > 1$ arbitrary. It turns out to be most convenient to do so in terms of the sums $S(h, t, m)$ defined in (4). This allows them to be compared, under GRH, with Wagstaff's evaluation of $N_{g,t}(x)$ ([11, Theorem 2.2]). The latter evaluation requires several arithmetically complicated cases to be distinguished. This makes the comparison process rather involved. Theorem 1 then follows on noticing that in all cases we have equality up to the required error term.

In the proof of Theorem 1 given here we start out by considering $f_{\gamma,t}(G)$, which is defined as $f_{\gamma,t}(G) = 1$ if $t|[G : \langle\gamma\rangle]$ and $f_{\gamma,t}(G) = 0$ otherwise. The analog of (5) is (7), which, being arithmetically easier, is less complicated to work with. Proceeding as before we end up concluding that the 'linear' and 'quadratic' contribution taken together yield an asymptotically exact heuristic for $R_{g,t}(x)$. The comparison process is easier here and only requires evaluating $[\mathbb{Q}(\zeta_{kt}, g^{1/kt}) : \mathbb{Q}]$ instead of $A(g, t)$. By means of (10) the heuristic for $R_{g,t}(x)$ is easily 'pushed through' to a heuristic for $N_{g,t}(x)$. In this approach one bypasses the use of the sums $S(h, t, m)$ and the condition $((p-1)/t, h_t) = 1$ comes up naturally (Lemma 14 with $G = (\mathbb{Z}/p\mathbb{Z})^*$ and thus $n = p - 1$), instead of in a somewhat ad hoc way.

4 On t-divisible residual indices

Let $g \in \mathbb{Q}\backslash\{-1,0,1\}$. Let $R_{g,t}$ be the set of primes p with $t|r_g(p)$ and $R_{g,t}(x)$ the number of primes $p \le x$ in $R_{g,t}$.

We study the set $R_{g,t}$ by two different methods. On the one hand by characters of $(\mathbb{Z}/p\mathbb{Z})^*$, where p runs over the primes and on the other hand by algebraic and analytic number theory. Thus in Lemma 1 we set up a character identity. In Lemma 4 the sum, $M_{g,t}(x)$, of the contributions of the 'linear' and 'quadratic' characters to $R_{g,t}(x)$ is evaluated, invoking Lemma 3. The asymptotic behaviour of $M_{g,t}(x)$ is determined (in Lemma 8) and compared with the asymptotic behaviour of $R_{g,t}(x)$ as resulting from number theory (given in Lemma 9). This comparison then shows that the total contribution of the characters of third and higher order is of lower order than the contribution of the characters of first and second order (Theorem 3).

Lemma 1 *Let G be a finite cyclic group of order n, $t|n$ and $\gamma \in G$. Put $f_{\gamma,t}(G) = 1$ if $t|[G:\langle\gamma\rangle]$ and $f_{\gamma,t}(G) = 0$ otherwise. Then*

$$f_{\gamma,t}(G) = \frac{1}{t}\sum_{d|t}\sum_{\mathrm{ord}\chi=d}\chi(\gamma), \tag{7}$$

where the inner summation is over the multiplicative characters on G having order precisely d.

Proof. First consider the case where t is squarefree. On noting that $\sum_{\mathrm{ord}\chi=d}\chi(\gamma)$ is multiplicative in d, we obtain

$$f_{\gamma,t}(G) = \frac{1}{t}\prod_{p|t}\left(1 + \sum_{\mathrm{ord}\chi=p}\chi(\gamma)\right).$$

If $p|[G:\langle\gamma\rangle]$, then $\sum_{\mathrm{ord}\chi=p}\chi(\gamma) = p-1$ and hence $f_{\gamma,t}(G) = 1$ if $t|[G:\langle\gamma\rangle]$. On the other hand, if $t \nmid [G:\langle\gamma\rangle]$, then there is a prime q such that $q|t$ and $q \nmid [G:\langle\gamma\rangle]$. Then $\sum_{\mathrm{ord}\chi=q}\chi(\gamma) = -1$ and $f_{\gamma,t}(G) = 0$. The general case is not so immediate, but easily dealt with on using Proposition 5 of [7]. □

Lemma 1 and its proof can also be formulated in terms of Ramanujan sums

$$c_d(n) := \sum_{\substack{1\le k\le d\\(k,d)=1}} e^{\frac{2\pi ikn}{d}}.$$

Lemma 2 *We have $f_{\gamma,t}(G) = \frac{1}{t}\sum_{d|t}c_d([G:\langle\gamma\rangle])$.*

Proof. Suppose $e|r$, then by [4, p. 79] the sum $\sum_{d|r}c_d(e)$ equals r if $e=r$ and zero otherwise. Now let e and r be arbitrary. On noticing that $\sum_{d|r}c_d(e) = \sum_{d|r}c_d((e,r))$ and invoking the latter result, we see that $\sum_{d|r}c_d(e)$ equals r if $r|e$ and zero otherwise. On putting $r=t$ and $e=[G:\langle\gamma\rangle]$ the result follows. □

`Remark`. By Möbius inversion it follows from Lemma 1 and Lemma 2 that

$$\sum_{\mathrm{ord}\chi=d}\chi(\gamma)=\sum_{\delta|d}\delta f_{\gamma,\delta}(G)\mu(\frac{d}{\delta})=c_d([G:\langle\gamma\rangle]).$$

For p prime put $G=(\mathbb{Z}/p\mathbb{Z})^*$ and $\psi_d(p)=\sum_{\mathrm{ord}\chi=d}\chi(g)$.

Lemma 3 *Adopt the notations and assumptions of Theorem 1. Put*

$$\epsilon_2=\begin{cases}0 & \text{if } \tau\le e;\\ 1 & \text{if } \tau>e.\end{cases}$$

Assume that $p\equiv 1(\mathrm{mod}\ (h,t))$. *If* $g>0$, *then* $\sum_{d|(h,t)}\psi_d(p)=(h,t)$. *If* $g<0$, *then*

$$\sum_{d|(h,t)}\psi_d(p)=\begin{cases}(h,t) & \text{if } p\equiv 1(\mathrm{mod}\ 2(h,t));\\ 0 & \text{otherwise.}\end{cases}$$

Assume that $p\equiv 1(\mathrm{mod}\ (2h,t))$. *If* $g>0$, *then*

$$\sum_{\substack{d|(2h,t)\\ d\nmid h}}\psi_d(p)=\epsilon_2(\frac{d(g_0)}{p})(h,t).$$

If $g<0$, *then*

$$\sum_{\substack{d|(2h,t)\\ d\nmid h}}\psi_d(p)=\epsilon_2(-1)^{\frac{p-1}{2^{e+1}}}(\frac{d(g_0)}{p})(h,t).$$

Proof. Straightforward on using Lemma 15 of [7] to evaluate $\psi_d(p)$ in each of the four cases, cf. the proof of Lemma 16 of [7]. □

Put

$$L_{g,t}(x)=\frac{1}{t}\sum_{\substack{p\le x\\ p\equiv 1(\mathrm{mod}\ t)}}\sum_{d|(h,t)}\psi_d(p)\text{ and }Q_{g,t}(x)=\frac{1}{t}\sum_{\substack{p\le x\\ p\equiv 1(\mathrm{mod}\ t)}}\sum_{\substack{d|(2h,t)\\ d\nmid h}}\psi_d(p).$$

Using Lemma 1, the definitions of $\psi_d(p)$, $L_{g,t}(x)$ and $Q_{g,t}(x)$, we conclude that

$$R_{g,t}(x)=L_{g,t}(x)+Q_{g,t}(x)+\frac{1}{t}\sum_{\substack{p\le x\\ p\equiv 1(\mathrm{mod}\ t)}}\sum_{\substack{d|t\\ d\nmid 2h}}\psi_d(p).$$

Although we are interested only in $M_{g,t}(x):=L_{g,t}(x)+Q_{g,t}(x)$, $L_{g,t}(x)$ and $Q_{g,t}(x)$ are of rather different nature and hence we are forced to consider them by themselves. Roughly speaking $L_{g,t}(x)$ gives the contribution of those characters such that $\chi(g)=1$ for all characters χ having the same order and $Q_{g,t}(x)$ of those such that $\chi(g)$ reduces to a quadratic character for all χ having the same order.

Let K be an arbitrary algebraic number field and let $P_K(x)$ denote the number of rational primes $p\le x$ that split completely in K. On using the previous lemma and noticing that

$$\sum_{\substack{p\le x\\ p\equiv 1(\mathrm{mod}\ t)}}(\frac{d(g_0)}{p})=2P_{\mathbb{Q}(\zeta_t,\sqrt{g_0})}(x)-\pi(x;t,1),$$

one finds after some computation:

Lemma 4 *Define $M_{g,t}(x) := L_{g,t}(x) + Q_{g,t}(x)$ and $t_h = t/(t,h)$. If $g > 0$, then*

$$M_{g,t}(x) = \begin{cases} \pi(x;t,1)/t_h & \text{if } \tau \le e; \\ 2P_{\mathbb{Q}(\zeta_t,\sqrt{g_0})}(x)/t_h & \text{if } \tau > e. \end{cases}$$

If $g < 0$, then

$$M_{g,t}(x) = \begin{cases} \pi(x;2t,1)/t_h & \text{if } \tau \le e; \\ \{4P_{\mathbb{Q}(\zeta_{2t},\sqrt{g_0})}(x) - 2P_{\mathbb{Q}(\zeta_t,\sqrt{g_0})}(x) + 2\sum_{\substack{p\le x \\ p\equiv 1 (\mathrm{mod}\ t) \\ p\not\equiv 1(\mathrm{mod}\ 2t)}} 1\}/t_h & \text{if } \tau = e+1; \\ 2P_{\mathbb{Q}(\zeta_t,\sqrt{g_0})}(x)/t_h & \text{if } \tau > e+1. \end{cases}$$

We will use Lemma 4 to deduce Lemma 8, which gives the asymptotic behaviour of $M_{g,t}(x)$. In order to do so we need a result due to Siegel and Walfisz and the prime ideal theorem (due to Landau).

Lemma 5 [9, Satz 4.8.3]. *Let C be a fixed real number. Then the estimate*

$$\pi(x;d,a) := \sum_{\substack{p\le x \\ p\equiv a(\mathrm{mod}\ d)}} 1 = \frac{\mathrm{Li}(x)}{\varphi(d)} + O(xe^{-c_1\sqrt{\log x}})$$

holds uniformly for all integers a and d such that $(a,d) = 1$ and $1 \le d \le \log^C x$, with c_1 some positive constant.

Lemma 6 [2]. *Let K be an algebraic number field. Let $\pi_K(x)$ denote the number of prime ideals of norm at most x. There exists $c_2 > 0$ such that*

$$\pi_K(x) = \mathrm{Li}(x) + O(xe^{-c_2\sqrt{\log x}}).$$

Corollary 1 *Let $P_K(x)$ denote the number of rational primes $p \le x$ that split completely in the number field K. If K is normal, then*

$$P_K(x) = \frac{\mathrm{Li}(x)}{[K:\mathbb{Q}]} + O(xe^{-c_2\sqrt{\log x}}).$$

`Remark`. A more complicated but sharper error term was obtained by Mitsui [5]. If the Riemann hypothesis holds for the Dedekind zeta-function $\zeta_K(s)$, then it can be shown [3] that the error is of order $O(\sqrt{x}\log(d(K)x^{[K:\mathbb{Q}]}))$, where $d(K)$ denotes the absolute value of the discriminant of K.

Also we need an explicit evaluation of the field degree $[\mathbb{Q}(\zeta_t, g^{1/t}) : \mathbb{Q}]$, which is given in the next lemma.

Lemma 7 *Write $t_h = t/(t,h)$ and $[\mathbb{Q}(\zeta_t, g^{1/t}) : \mathbb{Q}] = \varphi(t)t_h/\nu$. If $g > 0$, we have $\nu = 2$ if t_h is even and $d(g_0)|t$; otherwise $\nu = 1$. Now suppose $g < 0$. If t is odd, then $\nu = 1$. If t is even and t_h is odd, then $\nu = 1/2$. If t is even and $t_h \equiv 2(\mathrm{mod}\ 4)$, then*

$$\nu = \begin{cases} 2 & \text{if } d(g_0) \nmid t \text{ and } d(g_0)|2t; \\ 1 & \text{otherwise.} \end{cases}$$

If t is even and $4|t_h$, then $\nu = 2$ if $d(g_0)|t$ and $\nu = 1$ otherwise.

Proof. This is [11, Proposition 4.1], with the condition $t \equiv 2 (\mathrm{mod}\ 4)$ and $d(-g_0)|t$ or $t \equiv 4(\mathrm{mod}\ 8)$ and $d(2g_0)|t$ replaced by the equivalent condition $d(g_0) \nmid t$ and $d(g_0)|2t$. □

With the three latter results in hand, we can now prove the following lemma.

Lemma 8 *Let C be a fixed real number. Then for some $c_3 > 0$ the estimate*

$$M_{g,t}(x) = \frac{\mathrm{Li}(x)}{[\mathbb{Q}(\zeta_t, g^{1/t}) : \mathbb{Q}]} + O(xe^{-c_3\sqrt{\log x}})$$

holds uniformly for all t with $1 \le t \le (\log^C x)/d(g_0)$.

Proof. The primes p that split completely in $\mathbb{Q}(\zeta_t, \sqrt{g_0})$ are precisely the primes p satisfying $p \equiv 1(\mathrm{mod}\ t)$ and $(d(g_0)/p) = 1$. By the law of quadratic reciprocity these primes are precisely those in a union of residue classes of modulus at most $4d(g_0)t$. This means we can invoke Lemma 5. The natural density of the primes that split completely in $\mathbb{Q}(\zeta_t, \sqrt{g_0})$ is given by Lemma 1 as $1/[\mathbb{Q}(\zeta_t, \sqrt{g_0}) : \mathbb{Q}]$. The field degree $[\mathbb{Q}(\zeta_t, \sqrt{g_0}) : \mathbb{Q}]$ is well-known to be $2\varphi(t)$ if $d(g_0) \nmid t$ and $\varphi(t)$ otherwise. We obtain the assertion of the lemma with $\mathrm{Li}(x)/[\mathbb{Q}(\zeta_t, g^{1/t}) : \mathbb{Q}]$ replaced by $\mathrm{Li}(x)/c_{t,g}$, where $c_{t,g}$ is an easily explicitly evaluated constant. On comparing the values of $c_{t,g}$ with those of $[\mathbb{Q}(\zeta_t, g^{1/t}) : \mathbb{Q}]$ as given in Lemma 7, it is seen that $c_{t,g} = [\mathbb{Q}(\zeta_t, g^{1/t}) : \mathbb{Q}]$. □

The primes in $R_{g,t}$ are easily characterized algebraically. They are precisely the primes p satisfying $p \equiv 1(\mathrm{mod}\ t)$ and $g^{(p-1)/t} \equiv 1(\mathrm{mod}\ p)$. But these are precisely the primes splitting completely in $\mathbb{Q}(\zeta_t, g^{1/t})$ and thus $R_{g,t}(x) = P_{\mathbb{Q}(\zeta_t, g^{1/t})}(x)$. By Corollary 1 the following result then follows.

Lemma 9 *There exists $c_4 > 0$ such that*

$$R_{g,t}(x) = \frac{\mathrm{Li}(x)}{[\mathbb{Q}(\zeta_t, g^{1/t}) : \mathbb{Q}]} + O(xe^{-c_4\sqrt{\log x}}).$$

Comparison of Lemma 8 and Lemma 9 yields:

Theorem 3 *We have $R_{g,t}(x) = M_{g,t}(x) + O(xe^{-c_5\sqrt{\log x}})$, for some $c_5 > 0$.*

This theorem can be loosely phrased as stating that only the contributions of the 'linear' and 'quadratic' characters are responsible for the asymptotic behaviour of $R_{g,t}(x)$. That $M_{g,t}(x)$ and $R_{g,t}(x)$ are so closely related comes perhaps as a surprise, but in the next subsection we give a heuristic approach to $R_{g,t}(x)$ that will yield $M_{g,t}(x)$ as outcome.

4.1 Heuristic approach to $R_{g,t}(x)$

Let us first consider the case $g = g_0^h$. Then g is a priori in G^h (with $G = (\mathbb{Z}/p\mathbb{Z})^*$). We are interested in the case where g satisfies $t|[G : \langle g \rangle]$. Note that if $t|[G : \langle g \rangle]$, then $p \equiv 1(\mathrm{mod}\ t)$. If $t|p - 1$, then the elements of residual index t are all in G^t. The probability of finding g, given our a priori knowledge, in G^t equals $|G^h \cap G^t|/|G^h|$. The latter quotient is the density of elements in G^h having residual index divisible by t and is easily computable, also in the case where G is an arbitrary cyclic group.

Lemma 10 *Let G be a finite cyclic group of order n and let t and h be arbitrary with $t|n$. Then*

$$\rho_{1,*,t}(G) := \frac{|G^h \cap G^t|}{|G^h|} = \frac{(t,h)}{t} = \frac{1}{t_h}.$$

Heuristically we might expect that $R_{g,t}(x)$ behaves as $\sum_{\substack{p\le x\\ p\equiv 1(\text{mod } t)}} \rho_{1,*,t}((\mathbb{Z}/p\mathbb{Z})^*)$, that is as $\pi(x;t,1)/t_h$. Indeed, by Lemma 4 and Theorem 3 it does, except when $\tau > e$ and $d(g_0)|t$. Hence let us try to refine this heuristic. Suppose we know the value of the Legendre symbol $(d(g_0)/p)$. This improves our a priori knowledge and leads one to alter our group theoretical quotient. Let γ be a generator of G, thus $G = \langle\gamma\rangle$. Let n be the order of G. If $t|n$ we make the definitions

$$\rho_{1,1,t}(G) := \frac{|\{\gamma^{(\text{even})h}\} \cap G^t|}{|\{\gamma^{(\text{even})h}\}|} \left(= \frac{|G^{2h} \cap G^t|}{|G^{2h}|} \right) \text{ and } \rho_{1,-1,t}(G) := \frac{|\{\gamma^{(\text{odd})h}\} \cap G^t|}{|\{\gamma^{(\text{odd})h}\}|}.$$

If $t \nmid n$ we put $\rho_{1,1,t}(G) = \rho_{1,-1,t}(G) = 0$. Notice that if $(d(g_0)/p) = 1$, then the reduction of $g(\text{mod } p)$ is in $\{\gamma^{(even)h}\}$, otherwise it is in $\{\gamma^{(odd)h}\}$. We expect that a better heuristic for $R_{g,t}(x)$ is $H_{g,t}(x) := \sum_{p\le x} \rho_{1,(d(g_0)/p),t}((\mathbb{Z}/p\mathbb{Z})^*)$. Using Lemma 10 one deduces

$$\rho_{1,1,t}(G) = \frac{(2h,t)}{t} \text{ and } \rho_{1,-1,t}(G) = \frac{2(h,t)}{t} - \frac{(2h,t)}{t}.$$

In case $\tau \le e$ this reduces to $\rho_{1,1,t}(G) = \rho_{1,-1,t}(G) = t_h^{-1}$ and hence the naive heuristic yielding (as before), $H_{g,t}(x) = \pi(x;t,1)/t_h$. If $\tau > e$, then $\rho_{1,1,t}(G) = 2/t_h$ and $\rho_{1,-1,t}(G) = 0$, yielding $H_{g,t}(x) = 2P_{\mathbb{Q}(\zeta_t,\sqrt{g_0})}(x)/t_h$. By Lemma 4 we conclude that $H_{g,t}(x) = M_{g,t}(x)$ in case $g > 0$.

Now suppose $g < 0$ (hence $g = -g_0^h$). We assume that n is even and denote by -1 the unique element of order 2 in G. The analog of Lemma 10 reads

Lemma 11 *Let G be a finite cyclic group of even order n and let t and h be arbitrary with $t|n$. Then*

$$\rho_{-1,*,t}(G) := \frac{|{-G^h} \cap G^t|}{|{-G^h}|} = \begin{cases} 0 & \textit{if } ord_2(n) = \tau \text{ and } \tau \le e; \\ t_h^{-1} & \textit{otherwise.} \end{cases}$$

If $t \nmid n$ define $\rho_{-1,1,t}(G) = \rho_{-1,-1,t}(G) = 0$. If $t|n$ we make the definitions

$$\rho_{-1,1,t}(G) = \frac{|\{-\gamma^{(\text{even})h}\} \cap G^t|}{|\{-\gamma^{(\text{even})h}\}|} \text{ and } \rho_{-1,-1,t}(G) = \frac{|\{-\gamma^{(\text{odd})h}\} \cap G^t|}{|\{-\gamma^{(\text{odd})h}\}|}.$$

We consider how good $H_{g,t}(x) := \sum_{p\le x} \rho_{-1,(d(g_0)/p),t}((\mathbb{Z}/p\mathbb{Z})^*)$ is as a heuristic for $R_{g,t}(x)$. To that end we evaluate $\rho_{-1,1,t}(G)$ and $\rho_{-1,-1,t}(G)$ first.

Lemma 12 *Suppose G is a cyclic group of even order n and $t|n$. Then*

$$\rho_{-1,1,t}(G) = \begin{cases} 0 & \textit{if } ord_2(n) = \tau \textit{ and } \tau \le e+1; \\ (2h,t)/t & \textit{otherwise.} \end{cases}$$

Furthermore,

$$\rho_{-1,-1,t}(G) = \begin{cases} 0 & \textit{if } ord_2(n) = \tau \textit{ and } \tau \ne e+1; \\ 0 & \textit{if } ord_2(n) \ge \tau+1 \textit{ and } \tau \ge e+1; \\ (2h,t)/t & \textit{otherwise.} \end{cases}$$

Proof. Let us consider the more difficult case of evaluating $\rho_{-1,-1,t}(G)$. The intersection $\{-\gamma^{(\text{odd})h}\} \cap G^t$ consists of those elements γ^α with $1 \le \alpha \le n$ satisfying both $\alpha \equiv n/2 + (h,n)(\text{mod }(2h,n))$ and $\alpha \equiv 0(\text{mod } t)$. The intersection is thus empty iff $n/2 + (h,n) \not\equiv 0(\text{mod }(2h,t))$. On using that $(2h,t)$ divides both n and $2(h,n)$ one infers that $(2h,t) \nmid n/2$ and $(2h,t) \nmid (h,n)$ implies that $(2h,t)$ divides $n/2+(h,n)$. Thus the intersection is empty iff either $(2h,t)|n/2$ and $(2h,t) \nmid (h,n)$ or $(2h,t) \nmid n/2$ and $(2h,t)|(h,n)$. Since $(2h,t)|2(h,n)$ we have that $(2h,t)|(h,n)$ iff $\text{ord}_2((2h,t)) \le \text{ord}_2((h,n))$. Similarly $(2h,t)|n/2$ iff $\text{ord}_2((2h,t)) \le \text{ord}_2(n)-1$. Recalling that $\text{ord}_2(n) \ge \tau$ (by assumption), $\text{ord}_2(h) = e$ and $\text{ord}_2(t) = \tau$, we deduce that the intersection is empty iff either $\text{ord}_2(n) = \tau$ and $\tau \ne e+1$ or $\text{ord}_2(n) \ge \tau + 1$ and $\tau \ge e+1$.

If the intersection is non-empty, then it consists of $n/\text{lcm}((2h,n),t)$, that is $n(2h,t)(2h,n)^{-1}t^{-1}$ elements, whereas $\{-\gamma^{(\text{odd})h}\}$ consists of $n/(2h,n)$ elements. The quotient of these two cardinalities is $(2h,t)/t$. □

For future use we make the definition $r_{g,t}(p) := t_h \rho_{\text{sgn}(g),(d(g_0)/p),t}((\mathbb{Z}/p\mathbb{Z})^*)$. Note that $r_{g,t}(p) \in \{0,1,2\}$. The evaluation of $\rho_{\pm1,\pm1,t}(G)$ yields the following more precise result for $r_{g,t}(p)$. (Recall that ϵ_1 and ϵ_2 are defined in Theorem 1, respectively Lemma 3.)

Lemma 13 *If $g > 0$ and $p \equiv 1(\text{mod } t)$, then $r_{g,t}(p) = 1 + \epsilon_2(d(g_0)/p)$. If $g < 0$ and $p \equiv 1(\text{mod } 2^{1-\epsilon_2}t)$, then*

$$r_{g,t}(p) = 1 + |\epsilon_1|(-1)^{\frac{p-1}{2^{e+1}}} \left(\frac{d(g_0)}{p}\right).$$

In all other cases $r_{g,t}(p) = 0$.

Thus,

$$\rho_{\text{sgn}(g),(d(g_0)/p),t}((\mathbb{Z}/p\mathbb{Z})^*) = r_{g,t}(p)/t_h. \tag{8}$$

Using Lemma 12 and Lemma 4 one easily infers that $H_{g,t}(x) = M_{g,t}(x)$. Thus, irrespective of the sign of g, we have

$$H_{g,t}(x) = \sum_{p \le x} \rho_{\text{sgn}(g),(\frac{d(g_0)}{p}),t}((\mathbb{Z}/p\mathbb{Z})^*) = \frac{1}{t_h} \sum_{\substack{p \le x \\ p \equiv 1(\text{mod } t)}} r_{g,t}(p) = M_{g,t}(x). \tag{9}$$

Using Theorem 3 we see that the 'quadratic' heuristic proposed here is actually asymptotically exact ! The 'linear' heuristic, on the other hand, is only asymptotically exact in some cases.

5 Equal residual indices

By inclusion and exclusion it follows that

$$N_{g,t}(x) = \sum_{k=1}^{\infty} \mu(k) R_{g,kt}(x) \tag{10}$$

Assuming the error terms to cancel sufficiently, we expect from Lemma 9 that

$$N_{g,t}(x) = A(g,t)\frac{x}{\log x} + o\left(\frac{x}{\log x}\right).$$

Unfortunately it seems out of reach of present day methods to prove the cancellation in the error terms. On assuming GRH, however, the individual error terms involved are all sufficiently small resulting in a total error term of $o(x/\log x)$, cf. Theorem 2.

5.1 Heuristics for equal residual indices

Just as we used the principle of inclusion and exclusion to study $N_{g,t}(x)$ in the previous section, we can use it to set up heuristics for equal residual indices. The analog $\sigma_{1,*,t}(G)$ of the 'linear' heuristic $\rho_{1,*,t}(G)$ is given and evaluated in the next lemma. Note that $\sigma_{1,*,t}(G)$ is the density of elements in G^h having residual index t.

Lemma 14 *Let G be a finite cyclic group of order n and $t|n$. We have*

$$\sigma_{1,*,t}(G) := \sum_{d|n/t} \mu(d) \frac{|G^h \cap G^{dt}|}{|G^h|} = \begin{cases} (h,t)\varphi(n/t)/n & \textit{if } (n/t, h_t) = 1; \\ 0 & \textit{otherwise.} \end{cases}$$

Proof. By Lemma 10 the sum under consideration equals

$$\frac{(h,t)}{t} \sum_{d|n/t} \frac{\mu(d)}{d} \frac{(h,dt)}{(h,t)}. \tag{11}$$

The argument of the latter sum is multiplicative and we find that it equals zero iff there is a prime divisor q of n/t satisfying $(h,qt) = q(h,t)$. This is the case iff $(n/t, h_t) > 1$. If $(n/t, h_t) = 1$, then we find that the sum under consideration equals $t_h^{-1} \prod_{q|n/t}(1 - 1/q) = (h,t)\varphi(n/t)/n$. □

For a cyclic group G of order n divisible by t let us define

$$\sigma_{\pm 1,\pm 1,t}(G) = \sum_{d|n/t} \mu(d) \rho_{\pm 1,\pm 1,dt}(G).$$

This reduces to $\sum_{d|(p-1)/t} \mu(d) r_{g,dt}(p)(h,dt)/(dt)$ in case $G = (\mathbb{Z}/p\mathbb{Z})^*$. The following result holds true (for notational convenience we denote $(h,t)\varphi((p-1)/t)/(p-1)$ by $\mu_{g,t}(p)$).

Lemma 15 *We have $\sigma_{\mathrm{sgn}(g),(d(g_0)/p),t}((\mathbb{Z}/p\mathbb{Z})^*) = w_{g,t}(p)\mu_{g,t}(p)$.*

Proof. There are several cases to be considered and we deal only with a more challenging one: $g < 0$ and $2|h_t$ (note that $2|h_t$ is equivalent with $\tau < e$). If $\text{ord}_2(p-1) = \tau$, then $\sigma_{(d(g_0)/p),t}((\mathbb{Z}/p\mathbb{Z})^*) = 0$, by Lemma 12. If $\text{ord}_2(p-1) \geq \tau+1$, that is $p \equiv 1(\text{mod } 2t)$, then by Lemma 12, $\sigma_{(d(g_0)/p),t}((\mathbb{Z}/p\mathbb{Z})^*)$ equals the sum in (11) but with the divisors d restricted by $\text{ord}_2(p-1) \geq \tau + \text{ord}_2(d) + 1$. This is nothing but the sum in (11) with $(p-1)/t$ replaced by $(p-1)/2t$. Thus if $((p-1)/2t, h_t) > 1$, then this sum is zero. If $((p-1)/2t, h_t) = 1$, then since h_t is even, $(p-1)/2t$ is odd and $\varphi((p-1)/2t) = \varphi((p-1)/t)$. Using this we see that the sum equals $2(h,t)\varphi((p-1)/2t)/(p-1) = 2\mu_{g,t}(p)$. It follows that if $g < 0$ and $2|h_t$, then $\sigma_{(d(g_0)/p),t}((\mathbb{Z}/p\mathbb{Z})^*)/\mu_{g,t}(p)$ equals 0 if $p \not\equiv 1(\text{mod } 2t)$ and 2 otherwise. These values match with $w_{g,t}(p)$.

In the remaining cases sums of the form (11) appear, but with d restricted to be even or odd. These sums are easily evaluated. □

Corollary 2 *We have* $\sum_{d|\frac{p-1}{t}} \mu(d) r_{g,dt}(p) \frac{(h,dt)}{dt} = w_{g,t}(p)(h,t)\frac{\varphi((p-1)/t)}{p-1}$.

The latter corollary expresses $w_{g,t}(p)$ in terms of $r_{g,*}(p)$'s. It is also possible to express $r_{g,t}(p)$ in terms of $w_{g,*}(p)$'s. To that end one has to realize that since $\rho_{1,*,t}(G)$ and $\sigma_{1,*,t}(G)$ are the fraction of elements in G^h having residual index divisible by t, respectively equal to t, we have $\rho_{1,*,t}(G) = \sum_{d|n/t} \sigma_{1,*,dt}(G)$. Similarly we have $\rho_{\pm 1,\pm 1,t}(G) = \sum_{d|n/t} \sigma_{\pm 1,\pm 1,dt}(G)$ and this leads, on invoking (8) and Lemma 15, to the following result.

Lemma 16 *We have* $r_{g,t}(p) = \frac{1}{t_h} \sum_{d|(p-1)/t} w_{g,dt}(p)(h,dt)\frac{\varphi(\frac{p-1}{dt})}{p-1}$.

The latter result can be proved also by something akin to the Möbius inversion formula:

Lemma 17 *Let t and n be arbitrary integers with $t|n$ and σ_1 and σ_2 be two arithmetic functions, then $\sum_{d|n/t} \sigma_1(dt) = \sigma_2(t)$ implies $\sigma_2(t) = \sum_{d|n/t} \mu(d)\sigma_1(dt)$ and vice versa.*

Proof. This result is a particular case of one of Rota's Möbius inversion formulae ([10, Corollary 1, p. 345]). If P is a locally finite partially ordered set (whose order relation is denoted by $\leq$) and $r(x)$ is a function on P and $s(x) = \sum_{x\leq y\leq z} r(y)$, then $r(x) = \sum_{x\leq y\leq z} \mu(x,y)s(y)$, where $\mu(x,y)$ is defined inductively as follows: $\mu(x,x) = 1$ for all $x \in P$. Suppose now that $\mu(x,z)$ has been defined for all z in the open segment $[x,y)$. Then set $\mu(x,y) = -\sum_{x\leq z<y} \mu(x,z)$. We apply this with P the partially ordered set of multiples of t dividing n, with $x = t$ and $z = n$. On noting that $\mu(d,dt) = \mu(d)$, the result follows. □

Using Lemma 15 we see that Theorem 1 can be interpreted as stating that the 'quadratic' heuristic for $N_{g,t}(x)$ is exact up to order $O(x \log\log x \log^{-2} x)$, under GRH. Indeed, if $N_{g,t}(x)$ tends to infinity with x, then under GRH we have that the 'quadratic heuristic' for $N_{g,t}(x)$ is asymptotically exact.

6 Proof of Theorem 1

In this section we present a proof of Theorem 1 that is rather different from the one given in [7].

Proof of Theorem 1. Let $C > 1$ be arbitrary. The implied constants below may depend on C, but on C only. Put $I_1 = \sum_{ktd(g_0)\le \log^C x} \mu(k)M_{g,kt}(x)$ and $I_2 = \sum_{ktd(g_0)>\log^C x} \mu(k)M_{g,kt}(x)$. We evaluate the (finite) sum $I := I_1 + I_2$ in two ways, yielding the proof on invoking Theorem 2.

By Lemma 8 we have

$$I_1 = \mathrm{Li}(x) \sum_{ktd(g_0)\le \log^C x} \frac{\mu(k)}{[\mathbb{Q}(\zeta_{kt}, g^{1/kt}) : \mathbb{Q}]} + O\left(\frac{x}{\log^C x}\right).$$

Since $r_{g,t}(p) \le 2$, it follows by (9) that $M_{g,t}(x) \le 2h\pi(x; t, 1)/t$ and thus $M_{g,t}(x) = 0$ for $x > t - 1$. From this, the latter estimate and the theorem of Brun-Titchmarsh, which states that the estimate $\pi(x; t, 1) = O(x/(\varphi(t)\log(x/t)))$ holds true uniformly for $1 \le t < x$, we find $I_2 = O(hd(g_0)x \log^{-C} x)$. Using Lemma 7 we find that

$$\sum_{ktd(g_0)>\log^C x} \frac{\mu(k)}{[\mathbb{Q}(\zeta_{kt}, g^{1/kt}) : \mathbb{Q}]} = O\left(\frac{hd(g_0)}{\log^C x}\right).$$

Combining the latter estimate with those for I_1 and I_2 gives

$$I = A(g, t)\mathrm{Li}(x) + O(hd(g_0)x \log^{-C} x). \tag{12}$$

On the other hand we have, on using (9) and Corollary 2,

$$\begin{aligned} I &= \sum_{k=1}^{\infty} \mu(k)M_{g,kt}(x) = \sum_{k=1}^{\infty} \mu(k)\frac{(h, kt)}{kt} \sum_{\substack{p\le x \\ p\equiv 1 (\mathrm{mod}\ kt)}} r_{g,kt}(p) \\ &= \sum_{\substack{p\le x \\ p\equiv 1 (\mathrm{mod}\ t)}} \sum_{k|\frac{p-1}{t}} \mu(k)\frac{(h, kt)}{kt} r_{g,kt}(p) = (h, t) \sum_{\substack{p\le x \\ p\equiv 1 (\mathrm{mod}\ t)}} w_{g,t}(p)\frac{\varphi((p-1)/t)}{p-1}. \end{aligned}$$

Theorem 1 now follows from the latter equality, (12) and Theorem 2. □

References

[1] C. Hooley, *Artin's conjecture for primitive roots*, J. Reine Angew. Math. **225** (1967), 209-220.

[2] E. Landau, Einführung in die elementare und analytische Theorie der algebraische Zahlen und der Ideale, Leipzig, Teubner, 1918.

[3] S. Lang, *On the zeta function of number fields*, Invent. Math. **12** (1971), 337-345.

[4] P.J. McCarthy, Introduction to Arithmetical Functions, Universitext, New York/Berlin, Springer-Verlag, 1986.

[5] T. Mitsui, *On the prime ideal theorem*, J. Math. Soc. Japan **20** (1968), 233-247.

[6] P. Moree, *On primes in arithmetic progression having a prescribed primitive root*, J. Number Theory **78** (1999), 85-98.

[7] P. Moree, *Asymptotically exact heuristics for (near) primitive roots*, J. Number Theory **83** (2000), 155-181.

[8] P. Moree, *Asymptotically exact heuristics for divisors of recurrences of second order*, in preparation.

[9] K. Prachar, Primzahlverteilung, New York/Berlin, Springer-Verlag, 1957.

[10] G.-C. Rota, *On the foundations of combinatorial theory I. Theory of Möbius functions*, Z. Wahrsch. Verw. Gebiete **2** (1964), 340-368.

[11] S.S. Wagstaff, *Pseudoprimes and a generalization of Artin's conjecture*, Acta Arith. **41** (1982), 141-150.

Korteweg-de Vries Instituut
Universiteit van Amsterdam
Plantage Muidergracht 24
1018 TV Amsterdam
The Netherlands.
e-mail: `moree@science.uva.nl`
homepage: http://staff.science.uva.nl/ ̃moree/